Supported Upgrade Paths for FortiOS™ Firmware

VERSION 5.0.13

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, March 15, 2016

Supported Upgrade Paths for FortiOS™ Firmware

01-540-199976-20140917

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-15	Updated to include 5.0.13. Added Downgrading issues and Failure of secondary WAN IP for admin access
2016-01-25	Web filter category removal and FortiManager added
2015-12-10	Correction of EOS date and Divergence for Release Notes section
2015-11-11	Corrected issue relating to upgrades to 5.0.11
2015-11-03	HA cluster not properly upgrading from 5.0.10 and change to the upgrade paths to avoid 5.0.10
2015-06-03	Added 2 new potential issue examples relating to Application Control and autoupdate override
2015-05-19	Updated to include 5.0.12
2015-04-07	Added new potential issue example, updated link to Product Life Cycle page
2015-01-27	Updated to include 5.0.11
2014-12-17	Updated to include 5.0.10
2014-12-08	New document template

Overview

Purpose of this Document

The goal of this document is to make it easier for you to upgrade your FortiGate unit by guiding you to the most likely intermediate firmware upgrades between your current version and the latest version of the firmware.The latest version being the one with the highest patch number in this version branch.

Since multiple versions of firmware are often developed at the same time, there are different versions of the upgrade path document, too. The title of the document will indicate which version of the firmware is the final destination of the recommended upgrade path options. Be sure that you are looking at the proper document for your objective. For instance, if your goal is to upgrade to the latest build of Version 5.0 looking at the Upgrade Path document for 5.2 might give you some options that would appear confusing.

Every time you perform an upgrade to the firmware you should carefully read the release notes of the firmware you are upgrading to. Release notes may include warnings or notices of exceptions. The release notes can be found on the support site in the same directory as the firmware. The Fortinet Support Site can be found at: https://support.fortinet.com.

For most devices these steps will show the path in steps from your current version to the latest Version, MR, and patch. The steps shown by the **Upgrade Steps Table** are not the only possible path, but they are supported and have been optimized to achieve the latest version of the firmware in the fewest steps.

Some older FortiGate hardware platforms do not have the resources to effectively use the most recent firmware versions and so do not support firmware updates past a certain version. To see if your device is affected by this check the Product Life Cycle page found at: https://support.fortinet.com/Information/ProductLifeCycle.aspx

Scope of the Document

The scope of this document is limited to recommended upgrade practices for the FortiOS firmware, which is used as the Operating System for the following products:

- FortiGate
- FortiWiFi
- FortiCarrier

This document does not include the upgrade paths for other Fortinet products such as:

- FortiManager
- FortiAnalyzer.

These products have their own upgrade path documentation.

Location of Upgrade Path documents for other products

Other upgrade path documents are available for the following products:

- FortiAnalyzer
- FortiManager

These documents are available from the Fortinet Customer Service & Support Site, found at https://support.fortinet.com, in the same directory as the firmware images and Release Notes.

Example links to Upgrade Guides:

- ftp://support.fortinet.com/FortiManager/v5.00/5.0/5.0.9/fortimanager-v5.0.9-upgrade-guide.pdf
- ftp://support.fortinet.com/FortiAnalyzer/v5.00/5.0/5.0.9/fortianalyzer-v5.0.9-upgrade-guide.pdf

The above links are examples only, as each firmware release for these products has its own document.

Product compatibility

This document does not include any references to release compatibility between Fortinet products. This is an issue that administrators of environments where different Fortinet products are used should be aware of. For instance, a specific version of FortiManager has a range of versions of FortiGate that it will be compatible with. If the FortiGates are upgraded without verifying that the FortiManager will be compatible with them, a situation could arise where the FortiManager will not be able to manage those newly upgraded FortiGates. On the other side of the equation, it is also possible to upgrade a FortiManager beyond the compatibility range of some of the older models of FortiGate.

If you have some older models of FortiGate that cannot be upgraded to current releases of firmware, and some brand new models of FortiGate that cannot run older firmware, the situation can arise where a single FortiManager will not be able to manage all of the FortiGates in the environment.This is an issue that the administrator needs to be aware of when making decisions about which firmware to run.

The compatibility between models is listed in the Release Notes of the products. These should be read and the environment should be planned out as a whole. It is possible that there is no one best option. The administrator will have to weigh the pros and cons of all of the variables and keep in mind what the most important requirements are for the environment.

Source Information

The initial source material for the development of the of the upgrade path table is the upgrade information section found in the Release Notes that are written up for each new build of the FortiOS firmware.

Each time a firmware build comes out it is tested for compatibility with some of the previous builds in both the current version and the version that preceded it. It is not, however necessarily tested with every single build in these two versions. The two, sometimes 3, versions that are supported at the time of release are developed in parallel and not in coordinated schedules so it is possible that the latest build in version 5 was developed long after a lower numbered build in version 5.2. In short, the upgrade testing is done against build that are available at the time of release. The upgrade steps may at times seem like they should be able to make larger jumps, but we will only included upgrade steps that have been tested and proven to work in those tests.

Divergence from the Release Notes

The FortiOS Upgrade path document is initially based on the contents of the Release Notes documents for the firmware, however, periodically, bugs or unexpected combinations of configurations are found that reveal situations the regular compatibility testing did not account for. These updates are incorporated into the Upgrade path document sometimes without being included into rewrites of the Release Notes. Even if these occur in a relative small portion of the cases they are incorporated into the path to make it as close to a "one path fits all" product as possible. While the paths set forth in the Release Notes will work most of the time for most configurations, the relatively small extra effort of an additional upgrade or two is considered a small price to pay for making sure hat the odds of a failed upgraded are as low as possible.

The other reason that the Supported Upgrade Paths document can appear different from the Release Notes is more in the form of a change in perspective. A Release Note's perspective is centered around the firmware version it is describing, so it reaches back to see how many builds back can be successfully upgraded to that version. The Upgrade Path document's perspective is taken from the device's current firmware version and attempts to find an efficient path forward.

Using the Upgrade Steps Table

We have tried to make using the table as simple as possible.

1. Determine which release is currently running on your FortiGate.
2. Find that release/build in the left hand column.
3. Upgrade from one release to the next based on the releases listed in that row.

Release numbers

Over the life of the firmware, the designation of the individual releases has changed but this document tries to make these designations as consistent and as easy to understand as possible.

Originally, the version designation was made up of a Version, possibly a major release within that version and possible a patch number within that major release. If one was trying to refer to one of the later patches in a later release of version 4 of the firmware it could be described as Version 4 MR 3 Patch 18.

To make writing the release name simpler a 'shorthand' developed using the pattern x.x.x. The numbers shown in the table below are an abbreviated form of the firmware version names.

1st Number	Version Number
2nd Number	MR Number
3rd Number	Patch Number

Example: 3.7.10 = Version 3.0 MR7 Patch 10

Recently, the longer version of describing the release was dropped in favor of the simplified format.So it is not FortiOS Version 5 MR 2 Patch 1. It is simply FortiOS 5.2.1. Within the table, the simplified version is always used when describing the path.

Build Numbers

In cases where there is no indication in the Web-based Manager what the version or build number is you can get the build number from the CLI by entering the command:

```
get system status
```

The value in the output of the command for “Branch point” will be the build number.

Max Value Issue

There is a range of builds where the maximum number of some of the objects was lowered, but then a few builds later was raised back up. If a configuration on a device was to have a number of these objects in excess of the lower value when doing an upgrade there could be issues and even data loss so the upgrade paths listed are designed to avoid upgrading into this lower max value range even though the Release Notes state that upgrading to these firmware builds is supported. When the release notes were written the act of increasing the values was not foreseen.

Standalone vs. HA configuration upgrades

If you read the Release Notes for the firmware upgrades you will notice a discrepancy between what the Release Notes say is possible for upgrades and what the Upgrade Steps Table shows.

In version 5 there is a difference in the steps between the patches depending on whether your FortiGate setup is in a standalone or an HA configuration. If you have a standalone setup you can upgrade from Patch 3 (5.0.3) directly to Patch 5 (5.0.5). However, if you are using an HA setup you need to add the intermediate step of going to Patch 4 (5.0.4), otherwise only the slave unit in the configuration will be upgraded to Patch 5.

In the table describing the steps in progressing through the upgrades the most cautious path is listed. This minimizes the possibility of confusion for somebody who has an HA cluster but reads the Release Notes, like everybody should, but was unaware of the known issue with the HA clusters.

Parallel Development

Development of the firmware is usually taking place on two paths at the same time.There is development taking place on the latest path, as well as the previous stable path. For instance if the latest path was 5.0.x then the previous stable path that would still be in development would be 4.3.x. This has 2 significant ramifications as far as upgrades are concerned. The first is that patches are still being built for each of these paths. The second is that because this development is taking place in parallel the number identifiers for the builds do not correspond directly with the sequence in which the builds come out.

Occasionally it will appear as if there are some odd jumps in the upgrade sequence. This has to do with the timing of releases of different versions of the firmware. Later builds of different versions can come out close together and so have a high likelihood of compatibility. This is why 5.0.6 can only upgrade up to 5.0.9 but 4.3.18 can upgrade to 5.0.12

Upgrade Methods

There are two methods of primary methods of upgrading the firmware through the GUI; either from a local file that has been previously downloaded or from the FortiGuard Network.

Upgrading from the Local Drive

When uploading the firmware from the local drive you must already have downloaded it from the Fortinet Support Site at https://support.fortinet.com/. Once you have logged in with the account ID and password that was created when registering the FortiGate, go to the Download section and select the icon for Firmware images. From there it is only a matter of selecting a product, such as a FortiGate and then selecting either HTTPS or FTP download. The layout of the firmware listing in both methods is a hierarchical tree. For instance if you wanted firmware 5.0.7 you would select the v5.00 directory, then the 5.0 directory, then the 5.0.7 directory. Once in the directory scroll down until find the correct firmware file name for your specific model. The select the file you wish to download.

The file names are intended to be helpful in determining the correct firmware for the model you need. Here are some of the conventions found in the file names.

- FGT_ = FortiGate
- FWF_ = FortiWiFi
- POE = Power over Ethernet
- VM32/VM64 = Virtual Machine versions of the firmware. The 32 and 64 referring to the bit architecture of the OS.

Firmware going directly on a Fortinet Device will have the `.out` extension.

Upgrading from the FortiGuard Network

The practice of strategically skipping some firmware versions to optimize the time and efficiency that it takes to get to the latest version is based on using the **Upgrade from: Local Hard Drive** option. If you try to use the **Upgrade from: FortiGuard Network** option you will notice that there are a limited number of firmware builds to which you may upgrade, or downgrade. This is because only options that are always going to be safe are available. The logic being that because there are no intermediate options possible, the next consecutive build will always be a safe option.

Because of this limitation in options, it means that you will not be able to use the **Upgrade from: FortiGuard Network** option to see all of the safe upgrade options. You will either have to use the included upgrade path table or study the Release Notes.

The builds that will be shown will most like be as follows:

For Upgrades:

- The next build in the current version track

For Downgrades:

- The previous build in the current version track.
- The latest build in the previous version track.

Upgrade Steps Table

Starting Version	Build #	Supported Steps to Latest Build of 5.0
End of Support Date for Version 5.0 = May 1, 2017		
5.0.13	322	Latest Build
5.0.12	318	► 5.0.13
5.0.11	310	► 5.0.13
5.0.10	305	► 5.0.13
5.0.9	292	► 5.0.11 ► 5.0.13
5.0.8	291	► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.7	3608	► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.6	271	► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.5	252	► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.4	228	► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.12
5.0.3	208	► 5.0.4 ► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.2	179	► 5.0.3 ► 5.0.4 ► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.13
5.0.1	147	► 5.0.3 ► 5.0.4 ► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.13
5.0	128	► 5.0.2 ► 5.0.3 ► 5.0.4 ► 5.0.7 ► 5.0.9 ► 5.0.11 ► 5.0.13
End of Support Date for Version 4.0 MR3 = March 19, 2017 (unless device supports FortiOS version 5.0, then it's March 19, 2014)		
4.0 MR3 patch18	689	► 5.0.13
4.0 MR3 patch17	688	► 5.0.13
4.0 MR3 patch16	686	► 5.0.13
4.0 MR3 patch15	672	► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
4.0 MR3 patch14	665	► 4.3.18 ► 5.0.13
4.0 MR3 patch13	664	► 4.3.18 ► 5.0.13
4.0 MR3 patch12	656	► 4.3.18 ► 5.0.13
4.0 MR3 patch11	646	► 4.3.18 ► 5.0.13
4.0 MR3 patch10	639	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch9	637	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch8	632	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch7	535	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch6	521	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch5	513	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch4	511	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch3	496	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch2	482	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3 patch1	458	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR3	441	► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 4.0 MR2 = April 1, 2013		
4.0 MR2 patch15	356	► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch14	353	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
4.0 MR2 patch13	349	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch12	346	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch11	342	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch10	338	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch9	334	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch8	328	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch7	324	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch6	320	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch5	315	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch4	313	► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch3	303	► 4.2.13 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch2	291	► 4.2.13 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2 patch 1	279	► 4.2.13 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR2	272	► 4.2.13 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 4.0 MR1 = August 24, 2012		
4.0 MR1 patch10	217	► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch9	213	► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch8	209	► 4.2.15 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
4.0 MR1 patch7	207	► 4.2.15 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch6	205	► 4.2.15 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch5	204	► 4.2.15 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch4	196	► 4.2.15 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch3	194	► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch2	192	► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1 patch1	185	► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 MR1	178	► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 4.0 = February 24, 2012		
4.0 patch4	113	► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 patch3	106	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 patch2	99	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0 patch1	98	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
4.0	92	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 3.0 MR7 = July 18, 2011		
3.0 MR7 patch10	754	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch9	753	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch8	752	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch7	750	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch6	744	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
3.0 MR7 patch5	741	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch4	740	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch3	737	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch2	733	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7 patch1	730	► 4.0.0 ► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR7	726	► 4.0.0 ► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 3.0 MR6 = February 4, 2011		
3.0 MR6 patch6	678	► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6 patch5	677	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6 patch4	673	► 4.0.4 ► 4.2.12 ► 4.3.6 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6 patch3	670	► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6 patch2	668	► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6 patch1	662	► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR6	660	► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 3.0 MR5 = July 3, 2010		
3.0 MR5 patch7	576	► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5 patch6	575	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5 patch5	574	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
3.0 MR5 patch4	572	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5 patch3	568	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5 patch2	565	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5 patch1	564	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR5	559	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 3.0 MR4 = December 29, 2009		
3.0 MR4 patch5	483	► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR4 patch4	480	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR4 patch3	479	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR4 patch2	477	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR4 patch1	475	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR4	474	► 3.5.7 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
End of Support Date for Version 3.0 MR3 = October 2, 2009		
3.0 MR3 patch14	418	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
3.0 MR3 patch13	417	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch12	416	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch11	416	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch10	415	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch9	413	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch8	411	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch7	410	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch6	406	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch5	405	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3 patch3	403	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
3.0 MR3	400	► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
The versions below are beyond end of support dates		
3.0 MR2	319	► 3.3.14 ► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13

Starting Version	Build #	Supported Steps to Latest Build of 5.0
3.0 MR1	247	► 3.2.0 ► 3.3.14 ► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
2.80.11	unknown	► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
2.80.X (X <11)	unknown	► 3.1.0 ► 3.2.0 ► 3.3.14 ► 3.4.5 ► 3.6.6 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13
2.50.10	unknown	► 2.80.11 ► 3.7.10 ► 4.1.0 ► 4.1.10 ► 4.3.5 ► 4.3.11 ► 4.3.18 ► 5.0.13

Potential Issues

Special Builds

Every now and then a "Special Build" is created for some specific purpose and some companies will put these into production. These special builds are not part of the normal upgrade path QA process and therefore have a greater risk of variance from what is normally expected in an upgrade. The table of the upgrade path is based on the Release Notes of the regular builds and may not have included testing against every special build as well. If you are running a special build, be even more cautious in upgrading than you would normally be.

Why read the Release Notes?

Previously in this document, it was recommended that before upgrading from one version of the firmware to a more recent one that the Release Notes be read. To give an indication of how important it is to read the Release Notes we will provide a sampling of some of the possible issues that may have to be dealt with upon upgrading.

To offer some clarification on the contents of this sampling, some of these issues were and are unavoidable because of the nature of the configurations of the FortiGate devices and the networks they were in. The reason for reading the Release Notes is to make sure that users are prepared for changes or potential outages that may occur so that the affected parties can be forewarned and the issues can be dealt with in a timely manner.

Sampling of upgrade issues

These are some issues, in no particular order, that have been brought to the attention of the Technical Assistance Center or the Documentation Team that could result during the course of a firmware upgrade.

Changing of Category Numbers

When looking at the FortiGuard Webfilter categories or Application categories in the GUI we see the nice easily understood names that indicate what they refer to but in the code of the firmware these categories are referenced by a integer and not a text string. Periodically the list of categories changes, whether by the number growing larger or smaller it doesn't matter. If the list changes then so do the values of objects in that list. If your policies are everything is wide open you are not likely to see an issue but if there are carefully crafted restrictions in place.

Web filter category removal and FortiManager

Sometimes an issue in the upgrade process will not effect the FortiGate itself but one of the other devices connecting to the FortiGate. This issue has the same flavor as the changing of Category numbers issue, but it differs in that it effects the FortiManager rather than the FortiGate itself.

In stead of changing the subject of a category, there is an instance where a category was completely removed from the list of categories. Firmware upgrades developed soon after the removal of the category sanitized the configuration file. Later firmware versions ignored the category if it was left in the configuration file. An upgrade

from 4.3.18 to 5.0.12 may leave the category in place, but this does not effect the FortiGate. However, if FortiManager, running a current version of its firmware, tries to work with a configuration file with the removed category in it, an error message is triggered.

To determine if your FortiGate may effect the FortiGate later on, run this simple check.

1. Save your configuration file to your hard drive
2. Open it in your favorite text or code editor.
3. Go to the "`config webfilter profile`" section.
4. Check to see if any of the webfilter profiles are set to perform an action on category 32 or if you're feeling lazy, do a search for "`set category 32`"

If you find a reference to category 32 and you have already upgraded past FortiOS 4.3.18, go into your configuration using the CLI, and remove any references to category 32 and proceed as close as possible to the upgrade path below.

To completely remove the chance of this effecting the FortiManager, use the following path when upgrading the FortiGate:

4.3.18 > 5.0.2 > 5.0.4 > 5.0.6 > 5.0.10

There appears to be a large number of intermediate steps where the sanitizing of the configuration file should be taking place. This is because references to the category were not removed all at once. It first disappeared from the GUI and then from various points within the CLI and the firmware code.

After reaching 5.0.10 proceed as normal.

This path was not added to the main table as it is a somewhat isolated case.

HA Virtual MAC Address Changes

HA virtual MAC addresses are created for each FortiGate interface based on that interface's index number. Between FortiOS 4.3 and 5.0 interface indexing changed. After upgrading a cluster to FortiOS 5.0 the virtual MAC addresses assigned to individual FortiGate interfaces may be different. You can use the get hardware nic <interface-name> command to view the virtual MAC address of each FortiGate interface.

The practical consequences of this could be seen in a situation where, in a very security conscious environment, there is some blocking or allowed traffic based on mac addresses. When the firewall's mac address is not on the list of allowed addresses any traffic going through the firewall is likely to be problematic.

Changing of Logging Settings

There was a case where upgrading a few builds too far, in a very specific scenario, changed a logging setting. When going from one of the 4.3 builds to one of the earlier 5.0 builds, VDOM policies that also had IPS profiles had one of the log setting change from logging all traffic to logging only UTM events. The upgrade path works in all other respects; it just a case of having to go through the affected policies and change the setting.

Oddly enough, if the upgrade had gone all the way to 5.0.8, the issue would not have occurred.

Familiar features removed or changed

While not an issue that will potentially stop the FortiGate from working, this issue will sometimes make it worthwhile to keep a close eye on the performance of your FortiGate after an upgrade to make sure everything is still doing what it was before the upgrade.

Example: Logtraffic function

For instance, when upgrading from 4.3 to version 5, the `logtraffic-start` function is disabled by default.

In version 4.3, the `extended-traffic-log`option in `config log [memory|disk|fortianalyzer|syslog] filter` controlled the session start logging. In version 5.0, this is controlled by `logtraffic-start` in the policy settings. If before the upgrade, the"extended-traffic-log" was enabled, the `logtraffic-start` in policy settings will be disabled. More often than not this is the default setting of after an upgrade..

While for some users the loss of this function may be inconsequential, to other users this function might be useful. This is another reason to read the Release Notes; checking to verify that features commonly used in your environment will be there after the upgrade.

Example: Disk Logging

In version 4.3, logging to the local disk was only possible if Disk Logging was enabled and by default, it was disabled. Enabling the feature could be done either through the GUI or the CLI. In 5.0, not only was the feature disabled by default, but enabling it could only be done through the CLI, and even then, a message would appear stating that Logging to the local disk could seriously impact performance and that it should not be done. Despite the warning, it was possible to override the disabling of the feature and turn it on. In version 5.2, for devices that had only a single hard drive, it is not possible to override the disabling of the feature. The feature is still part of the firmware and available through the CLI, just not to all models.

This brings up an interesting situation regarding the Release Notes. The fact that this feature was, by default disabled in 5.0 is mentioned in the Release Notes for 5.0. Because, the feature was still disabled between 5.0 and 5.2, although more strictly, it was not referred to the Release Notes for 5.2. If one is steadily upgrading the firmware on devices as they come out and reading the Release Notes, the evolution can be seen and this is not an issue. But making the jump from 4.3 to 5.2, and not reading the Release Notes of the intermediate firmware builds can lead to finding a feature missing that was expected to be there, if you hapen to have one of the specific models affected.

Example: config system autoupdate override

When upgrading to 5.0.12 the config systemautoupdate override function is removed. This feature was used to specify an alternate FDS server, usually a FortiManager, in the event that the FortiGuard Distribution Network (FDN) was unavailable.

Combination of variables that produce unexpected results

Every single possibility of variables cannot be tested, so every now and then a specific combination of variables will produce a side effect that is completely unexpected. Most of the time these side effects may not even be noticed but occasionally there can be some loss of functionality.

Example: Link Aggregation

One such example of this occurs when upgrading a FortiGate 600C from 4.3.18 to 5.0.11. If the FortiGate is configured to use Link Aggregation Control Protocol and an upgrade is done directly from 4.3.18 to 5.0.11, the VLANs under LACP will disappear and WiFi mash devices show up below it.

In order to prevent this from happening an upgrade to 5.0.7 needs to occur before the upgrade to 5.0.11. The reason that this path is not part of the table, is that this situation refers to only 1 model and with a particular configuration.

Example:Application Control

When upgrading from 5.0 to 5.2, there is a curious time delay on a side effect involving Application Control profiles. If you have an Application Control profile that has some categories included, as well as some individual Application Control signatures, and you upgrade from 5.0 to 5.2 everything will work as it did before. There is the slight side effect that you will no longer see the individual signatures in the GUI, but the functionality will still be there. The problem arises when the profile is actually edited. Editing the profile removes the individual signatures. The only way to correct the error is to manually enter them in again.

Downgrading issues

While most potential issues occur during the upgrade process there are occasional ones that can occur when downgrading firmware.

Generational incompatibility

Fortinet will sometimes produce different generations of the same model of device. Ideally, the firmware should not be downgraded to a version earlier that what it came with from the factory.

Example:

The FortiGate 3600C generation 3 came with a new NPU DDR chip that the first and second generations of the model did not have. The Support site has a firmware version 5.0.2 for the FortiGate 3600C.This would have been for the first generation of the model but the third generation of the model will not properly run this version of the firmware.

FORTINET®

High Performance Network Security

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.